NATIONAL FOREIGN INTELLIGENCE BOARD

NFIB-24.1/16
26 October 1977

3

MEMORANDUM FOR NATIONAL FOREIGN INTELLIGENCE BOARD

STATINTL

FROM: [redacted]
Executive Secretary

SUBJECT: Definitions Requested by the Senate Select Committee on Intelligence

1. The Senate Select Committee on Intelligence is drafting legislation intended to clarify the authority and responsibilities of the various departments and agencies performing intelligence functions. In support of this effort, the Committee has requested the Intelligence Community definitions of 26 listed terms.

2. The Director of Central Intelligence has requested that the NFIB Principals be provided the attached copy of the proposed definitions of these terms developed by an interagency group headed by [redacted] of the Intelligence Community Staff, as modified by the definitions of four terms contained in the draft Executive Order now being considered by the NSC Special Coordination Committee. The four definitions derived from what is now contained in the draft Executive Order are: foreign intelligence, foreign counterintelligence, international terrorist activities, and communications security.

STATINTL

3. In the interest of an expedited response to the Senate Committee, your concurrence or comments on the attached definitions is requested by Friday, 4 November 1977.

[redacted] STAT
Walter Elder

Attachment:
Proposed Definitions

MORI/CDF

DEFINITIONS OF INTELLIGENCE TERMS

INTELLIGENCE: A generic term which includes foreign intelligence and foreign counterintelligence. (See below.)

INTELLIGENCE ACTIVITIES: A generic term used to describe the efforts and endeavors undertaken by the departments, agencies, and elements comprising the Intelligence Community.

FOREIGN INTELLIGENCE (FI): The product of collection, processing and analysis of information relating to the capabilities, intentions and activities of foreign powers, organizations or persons, but not including foreign counterintelligence except for information on international terrorist activities.

FOREIGN COUNTERINTELLIGENCE: Information gathered and activities conducted to protect against espionage and other clandestine intelligence activities, sabotage, international terrorist activities or assassinations conducted for or on behalf of foreign powers, organizations or persons, and activities conducted abroad to protect national security information and its means of collection from detection by or disclosure to foreign powers, organizations or persons, but not including personnel, physical, document, or communications security programs.

TACTICAL INTELLIGENCE: That intelligence required by military commanders in the field to maintain the readiness of operating forces for combat operations and to support the planning and conduct of military operations under combat conditions.

INTERNATIONAL TERRORIST ACTIVITIES: Any activities which

(1) involve:
  (a) killing, causing serious bodily harm to or kidnapping one or more individuals, or
  (b) violent destruction of property, or
  (c) an attempt or credible threat to commit acts specified in subparagraphs (a) or (b) above; and
(2) appear intended to endanger a protectee of the Secret Service or the Department of State or to further political, social, or economic goals by:
  (a) intimidating or coercing a civilian population or any segment thereof, or
  (b) influencing the policy of a government or international organization by intimidation or coercion; or
  (c) obtaining widespread publicity for a group or its cause; and

(3) transcends national boundaries in terms of:
  (a) the means by which it is accomplished,
  (b) the civilian population, government or international organization it appears intended to coerce or intimidate, or
  (c) the locale in which its perpetrators operate or seek asylum.

DEPARTMENT(AL) INTELLIGENCE: Foreign intelligence produced and used within a governmental department or agency in order to meet unique requirements of the department or agency mission.

INTELLIGENCE-RELATED ACTIVITIES: Those activities specifically excluded from the National Foreign Intelligence Program which respond to departmental or agency tasking for time-sensitive information on foreign activities; respond to national Intelligence Community advisory tasking of collection capabilities which have a primary mission to support departmental or agency missions or operational forces; train personnel for intelligence duties; or are devoted to research and development of intelligence or related capabilities.

COMMUNICATIONS INTELLIGENCE (COMINT): Technical and intelligence information derived from intercept of foreign communications by other than the intended recipients. COMINT does not include the monitoring of foreign public media nor the intercept of oral or written communication obtained during the course of foreign counterintelligence investigations within the United States.

ELECTRONICS INTELLIGENCE (ELINT): Technical and intelligence information derived from foreign noncommunications electromagnetic radiations emanating from other than atomic detonation or radioactive sources.

FOREIGN INSTRUMENTATION SIGNALS INTELLIGENCE (FISINT): Information derived from the collection and processing of foreign telemetry, beaconry, and associated signals.

SIGNALS INTELLIGENCE (SIGINT): A category of intelligence information comprising all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, either individually or in combination, including as well nonimagery infrared and coherent light signals.

NONCOMMUNICATIONS EMANATIONS: That class of radiations which are emitted intentionally or unintentionally by electrical or electronic equipments for purposes other than communications, e.g., by radars, navigational aids, jammers, or remote control systems.

UNITED STATES SIGNALS INTELLIGENCE SYSTEM: An entity that is comprised of the National Security Agency (including assigned military personnel); those elements of the military departments and the Central Intelligence Agency performing signals intelligence activities; and those elements of any other department or agency which may from time-to-time be authorized by the National Security Council to perform signals intelligence activities during the time when such elements are so authorized.

COMMUNICATIONS SECURITY (COMSEC): The protection resulting from measures taken to deny unauthorized persons information derived from the national security-related communications of the United States Government and to ensure the authenticity of such telecommunications.

TRANSMISSION SECURITY (TRANSSEC): The component of communications security which results from all measures designed to protect transmissions from interception and from exploitation by means other than cryptanalysis.

EMISSION SECURITY (EMSEC): The component of communications security which results from all measures taken to deny to unauthorized persons information of value which might be derived from interception and analysis of compromising emanations from crypto-equipment and telecommunications systems.

PHYSICAL SECURITY: Physical measures--such as safes, vaults, perimeter barriers, guard systems, alarms and access controls--designed to safeguard installations against damage, disruption or unauthorized entry; information or material against unauthorized access or theft; and specified personnel against harm.

PERSONNEL SECURITY: The means or procedures, such as selective investigations, record checks, personal interviews, supervisory controls, designed to provide reasonable assurance that persons being considered for, or granted access to, classified information are loyal and trustworthy.

CRYPTOSECURITY: The component of communications security that results from the provision of technically sound cryptosystems and from their proper use.

CRYPTOLOGIC ACTIVITIES: The activities and operations involved in the production of signals intelligence and the maintenance of communications security.

CRYPTOLOGY: The branch of knowledge which treats the principles of cryptography and cryptanalytics and is used to produce signals intelligence and maintain communications security.

CODE: A cryptosystem in which the cryptographic equivalents (usually called "code groups"), typically consisting of letters or digits (or both) in otherwise meaningless combinations, are substituted for plaintext elements such as words, phrases, or sentences.

CIPHER: A cryptosystem in which the cryptographic treatment (i.e., the method for transforming plain text by predetermined rules to obscure or conceal its meaning) is applied to plaintext elements (such as letters, digits, polygraphs or bits) which either have no intrinsic meaning or are treated without regard to their meaning (e.g., if the element is a natural-language word).

CRYPTOSYSTEM: All associated items of cryptomaterial (e.g., equipments and their removable components which perform cryptographic functions, operating instructions, maintenance manuals) that are used as a unit to provide a single means of encryption and decryption of plain text, so that its meaning may be concealed. (In addition, code, cipher, and cryptographic systems include any mechanical or electrical device or method used for the purpose of disguising, authenticating, or concealing the contents, significance, or meanings of communications.)

NATIONAL INTELLIGENCE ESTIMATES (NIEs): Thorough assessments of situations in the foreign environment that are relevant to the formulation of foreign, economic, and national security policy, and project probable future courses of action and developments. They are structured to illuminate differences of view within the Intelligence Community, and are issued by the Director of Central Intelligence with the advice of the National Foreign Intelligence Board.